

EXPLOSION DE LA CYBERCRIMINALITE EN 2003

L'ensemble des études et rapports publiés entre fin 2003 et janvier 2004 par les spécialistes de la sécurité informatique fait clairement apparaître que 2003 a été une année « record » pour la cybercriminalité.

Ainsi, en 2003, L'*Internet Crime Complaint Center* américain n'a pas reçu moins de 120 000 plaintes pour des fraudes diverses sur Internet, soit une augmentation de 60% par rapport à 2002. Les fraudes et délits les plus constatés ont été :

- **Le détournement de données relatives à des cartes de crédit ;**
- **L'extorsion de fonds ;**
- **Le vol d'identité ;**
- **L'intrusion en vue de vol de données ;**

Si ces pratiques recourent celles déjà recueillies par le passé, les méthodes ont évolué et se sont sophistiquées avec le développement du « phising » (à prononcer « fishing »), une technique utilisant le « spamming ». En résumé, un « spam » est adressé à l'internaute depuis une adresse ressemblant à celle d'un commerçant ou d'un établissement en ligne connu en vue de récupérer des informations confidentielles.

Ce « phising » est pratiqué sur une très grande échelle puisque, rien que pour les deux dernières semaines de décembre 2003, les services compétents américains auraient détectés par moins de 60 millions de « phising spams » : la période (celle des achats de Noël...) était particulièrement favorable à ce type d'escroqueries. L'une des plus récentes manifestations du « phising » semble être, à la mi-janvier, une campagne de spams invitant des clients de la Citibank à se connecter sur un site web pour y vérifier l'état de leur compte : les personnes approchées étaient priées de vérifier si leur compte n'avait pas été utilisé à leur insu pour des opérations liées au blanchiment d'argent ou à diverses fraudes, sous peine de voir la banque bloquer leurs avoirs s'ils n'obtempéraient pas.

L'une des « nouveautés » de 2003 semble avoir été l'association du « phising » et de l'utilisation de « vers » informatiques permettant son automatisation et donnant donc à cette forme de cybercriminalité une ampleur jamais vue jusque-là. Des enquêtes du FBI ont fait apparaître que plusieurs milliers de ces courriers suspects provenaient de **Roumanie**, un pays qui fait figure de nouvelle plateforme internationale de la cybercriminalité. En 2003, du reste, l'activité du FBI et de Scotland Yard a permis l'arrestation de 60 programmeurs informatiques roumains employés par des bandes criminelles spécialisées dans le « phising ».

La « *Federal Trade Commission* », quant à elle, souligne que le vol d'identité sur Internet (qui permet par la suite d'effectuer des achats et des détournements en se

faisant passer pour un autre) n'aurait pas coûté moins de 48 milliards de dollars pour 2002 (les chiffres 2003 devraient être connus cet automne).

Les tendances constatées aux Etats-Unis se vérifient en Europe. Dans son dernier rapport, présenté à la mi-janvier, le CLUSIF (Club de la Sécurité des Systèmes informatiques français) souligne également la déferlante du « phising » en France et souligne le danger de l'alliance phiseurs/spammeurs. L'année 2003 a également été marquée par la recrudescence des attaques de réseaux par vers (SOBIG.E, SOBIG.F, BLASTER...).

Outre la Roumanie, d'autres pays pointés du doigt par les spécialistes sont la Chine et la Corée du Sud. Par ailleurs, certains experts estiment que le ver « Mydoom » aurait été créé en Russie par des pirates liés à la Mafia dans le but de repérer et d'utiliser des « portes dérobées » pour s'introduire dans les systèmes et y récupérer des données personnelles.

Les experts américains estiment que les chiffres de la fraude informatique devraient doubler en 2004...

esisc@esisc.org